IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: 175 OLD FRANKLIN ROAD STAHLSTOWN, PENNSYLVANIA 15687	Case No. 20-2012

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Detective H.W. Long, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 175 OLD FRANKLIN ROAD, STAHLSTOWN, PENNSYLVANIA 15687, hereinafter the "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Detective with the Raleigh County (West Virginia) Sheriff's Office. I have been employed with the Raleigh County Sheriff's Office since November 2012. As part of my current assignment, I am responsible for investigating crimes involving the sexual exploitation of children, which are violations of state and federal law. I am a member of the West Virginia Internet Crimes Against Children Task Force and have been since 2017. I am currently a member of the FBI Violent Crimes against Children (VCAC) Task Force. I have been assigned to the VCAC Task Force since approximately 2019, and as such have assisted in multiple investigations with the task force. The VCAC Task Force conducts investigations into child exploitation, child pornography, sexual assaults, sexual abuse and human trafficking. As part of my role with the VCAC Task Force I have been deputized by the United States Marshals Service.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not set forth all of my knowledge or the knowledge of others about this matter.

STATUTE UNDER INVESTIGATION

4. The investigation concerns violations of Title 18, United States Code, Sections 2422(b) relating to matters involving the enticement of minors to engage in illegal sexual activity. That statute makes it illegal for any person, through use of a means or facility of interstate commerce, to attempt to persuade, induce, entice, or coerce a minor to engage in sexual activity for which any person can be charged with a criminal offense.

PROBABLE CAUSE

5. On or about August 7, 2020, a law enforcement employee was acting in an undercover capacity ("UCO"). In that role, the UCO had created a Kik[1] account and was portraying a 13-year-old female. After the UCO persona joined a Kik chat room for West Virginia teens, the UCO received a message from user "Greg Inswpa," later identified as GREGORY THOMAS O'CONNOR. O'CONNOR's initial message read, "Hello, Saw you in the WVteen [sic] group and would love to chat" and shortly thereafter indicating he was looking for "a little discreet fun."

[1] Kik is a social messaging application that relies upon the Internet and cellular networks. It permits users to send and receive messages, images, and videos from other users. Kik also allows users to create and participate in group chat rooms.

6. During communication with O'CONNOR the UCO stated her age to be 13 on several different occasions. The UCO further indicated that she was located in Beckley, Raleigh County, West Virginia. O'CONNOR stated that he was 41 and married, expressing his hope that this would not be a problem for the minor. During the communications O'CONNOR also indicated he lived in Pennsylvania.

7. Initially messages between the UCO and O'CONNOR were intermittent and spread across approximately a week. Once the conversation became more frequent on approximately August 18, 2020, O'CONNOR quickly expressed his interest in traveling to Beckley to meet the minor in person and directed the conversation into sexual matters. He asked the minor about her sexual experiences, and upon learning that she was a virgin, he asked additional questions regarding her experiences with masturbation. O'CONNOR offered to "help teach you and give you some experience."

8. By August 24, 2020, O'CONNOR escalated the sexual nature of the conversation by requesting a telephone call with the UCO. A telephone call that day (which was recorded) lasted just under an hour and involved defendant directing the minor in detail about how to masturbate with details such as "get your fingers nice and wet and just gently rub your clit a little" and that she should slowly insert her finger into her vagina since she stated she had never done that before and feared it would hurt. He also stated he wanted to try to meet her in person soon and asked her to "promise me you're going to keep practicing [masturbation] at night and stuff when you're lying in bed?" He also suggested she look at the website porntube.com to learn more about sex.

9. On August 28, 2020, during another recorded phone call, the UCO again stated that she was only 13 years old and was afraid he'd view her as "a baby." He also stated, regarding when they met in person, that "hopefully you're comfortable, and like I said, if you, you know, if

you wanna look at my cock, or touch my cock, you know whatever, just to kind of get more familiar with things too you, you know whatever you want I'm more than happy to you know let you kind of dictate the pace."

10. O'CONNOR and the UCO arranged for O'CONNOR to travel on September 2, 2020, from his location in Pennsylvania to Beckley, West Virginia in order to meet in person to engage in sexual activity. On the morning of September 2, 2020, O'CONNOR sent the UCO a message on Kik indicating that he would have to reschedule their meeting. He informed her that he had driven to Fairmont, West Virginia, when he received a call from a construction job site that he was overseeing indicating that there was a problem. He stated that he had to travel back to Pennsylvania in order to deal with that issue. O'CONNOR sent her a picture of himself driving through Uniontown, Pennsylvania, in order to reassure the minor that he was not lying to her.

11. On approximately September 15, 2020, O'CONNOR told the UCO that it was "hot" that she was in 8th grade and the same age as his daughter. He further stated that "a couple of my daughters [sic] friends get me turned on as well." He later told the UCO that one of his daughter's friends (also the same age as his daughter and the UCO) was "very flirty" with him and described an occurrence that happened the last time that friend was at his house: "The last time she was over she was laying across my lap and had a very skimpy outfit on and had me turned on to the point that my cock was getting hard in my shorts. We had a blanket over us and I am pretty sure that she felt my cock getting hard and gave me a couple naughty glances. I am pretty sure she was kind of rubbing her leg across it on purpose. Out of all of her friends that would be the one that I could see something happening with if any of them. But it is a tough situation because we are really good friends with her parents and I have known her since she was like 3. So it would be very risky."

12. On approximately September 16, 2020, the UCO and O'CONNOR were discussing his trying to drive to see her the following week if he could get his schedule to work. He told her "I can't believe how my cock starts getting hard every time that I think about you. I guess I am just really turned on by the thought of being with someone so sexy." He further discussed that when they met in person "I am willing to try whatever you want to do. Just want to make sure that you are comfortable telling me what you want or what you like. I want you to be able to tell me if something is enjoyable, not enjoyable, or if something makes you feel like you don't like it. I just want you not to be afraid to be vocal with me. So I know that I am making you happy and feel good. And remember, it's not all about just jumping into getting a cock inside of you. It is about enjoying the whole sexual process. Foreplay, kissing, touching, etc. So I don't want you to just feel like you have to jump right into intercourse." But he later added that "I can't even begin to tell you how hot and erotic the thought of you and I having sex is to me."

13. Conversations between the UCO and O'CONNOR are still ongoing at this time.

14. As part of the investigation, law enforcement served an administrative subpoena on Verizon Wireless to obtain the subscriber information for the telephone number that O'CONNOR had used to engage in telephone calls with the UCO. The subpoena return indicated that the account holder was Gregory O'Connor with an address of 175 OLD FRANKLIN ROAD, STAHLSTOWN, PENNSYLVANIA 15687. A Pennsylvania driver's license issued to a Gregory O'Connor at the same address included a photograph that appeared to be the same person in the photographs sent to the UCO by O'CONNOR. The investigation further revealed that Gregory O'Connor in Stahlstown owned a construction company, corroborating his statement that he had to cancel his meeting with the UCO due to a problem at a construction site.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

15. This application seeks permission to search the PREMISES for O'CONNOR's cellular telephone, further identified in Attachment B, and the information located on said cellular telephone for certain records, which are also described further in Attachment B. Thus, the warrant applied for would authorize the seizure of an electronic storage medium and the potential copying of electronically stored information, all under Rule 41(e)(2)(B).

16. *Probable cause.* I submit that there is probable cause to believe that O'CONNOR's cellular telephone, as described in Attachment B, will be located at his residence, the PREMISES. Cellular telephones are personal devices that are typically kept on one's person or in one's residence when one is at home. To the extent that O'CONNOR is present at the PREMISES and his cellular phone is not located on his person, probable cause would exist to believe that it would be located on the PREMISES.

17. I submit that if O'CONNOR's cellular telephone, as identified in Attachment B, is found on the PREMISES, there is probable cause to believe the records described in Attachment B will be stored on that cellular phone, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can potentially be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Wholly apart from user-generated files, cellular telephones contain electronic evidence of how a phone has been used, what it has been used for, where it has been used, and who has used it.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cellular telephone was used, the purpose of its use, who used it, and when and where it was used. There is probable cause to believe that this forensic electronic evidence will be on O'CONNOR's cellular telephone, as identified in Attachment B, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the times the device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, and internet history) can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, cellular telephones frequently contain information that log: user account session times and durations, GPS and other location data, and the IP addresses or WiFi networks through which the cellular telephone accessed networks and the internet. Such information allows investigators to understand the chronological context of cellular telephone access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular phone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The geographic and timeline information described herein may either inculpate or

exculpate the user. Last, information stored within a cellular telephone may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within the cellular telephone may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., deleting only text messages from a potential minor victim but not from other individuals).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how the device was used, the purpose of its use, who used it, and when and where it was used.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

19. *Necessity of seizing or copying entire computers or storage media*. Generally the seizure of information stored on a cellular telephone requires the seizure of the physical storage media and later off-site review consistent with the warrant. Seizure is often necessary to ensure

the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Cellular telephones can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of cellular telephone hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

20. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

O'CONNOR's cellular telephone, as further described in Attachment B, and would authorize a later review of the media or information contained on that cellular telephone consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

21. This warrant also permits law enforcement to compel GREGORY THOMAS O'CONNOR to unlock any cellular telephone owned and utilized by O'CONNOR subject to seizure pursuant to this warrant located on his person or elsewhere at the PREMISES and requiring biometric access. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is

found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that the cellular telephone identified in Attachment B will be found during the search. The passcode or password that would unlock such device subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted

Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter devices owned and utilized by GREGORY THOMAS O'CONNOR that are subject to seizure pursuant to this warrant (as further identified in Attachment B) and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of GREGORY THOMAS O'CONNOR to the fingerprint scanner of the devices found at the PREMISES; (2) hold the devices found at the PREMISES in front of the face of GREGORY THOMAS O'CONNOR and activate the facial recognition feature; and/or (3) hold the devices found at the PREMISES in front of the face of GREGORY THOMAS O'CONNOR and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. Only devices owned and utilized by O'CONNOR are subject to this authorization, and such authorization on-site is limited to only allow use of biometric data to determine which phone is the specific phone identified in Attachment B for seizure; once such phone has been identified, no additional phones owned and utilized by O'CONNOR may be unlocked by biometric data. The proposed warrant does not authorize law enforcement to compel that GREGORY THOMAS O'CONNOR state or otherwise provide the password or

any other means that may be used to unlock or access any devices owned or utilized by him. Moreover, the proposed warrant does not authorize law enforcement to compel GREGORY THOMAS O'CONNOR to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,
s/ H.W. Long

_____

H.W. Long
Detective
Raleigh County (WV) Sheriff's Office

Sworn and subscribed to me, by telephone pursuant to Fed. R. Crim. P. 4.1(b)(2)(A), this 2nd day of October, 2020.

_____

MAUREEN P. KELLY
UNITED STATES MAGISTRATE JUDGE